

AMENDMENTS TO THE CLAIMS

- 1 1. (original) A method of controlling access of network management requests directed
2 to one or more network devices that participate in a virtual private network, the
3 method comprising the computer-implemented steps of:
4 receiving a request to carry out a management protocol operation;
5 determining an identifier of a virtual private network in the request;
6 identifying, among a plurality of managed objects, a subset of objects that requests
7 associated with the virtual private network are permitted to access; and
8 providing the request with access to only the subset of objects.
- 1 2. (original) A method as recited in Claim 1, further comprising the steps of providing,
2 at one of the network devices, a mapping of a plurality of identifiers of virtual private
3 networks to corresponding views of subsets of managed objects.
- 1 3. (currently amended) A method as recited in Claim 1, further comprising the steps of
2 providing, at one of the network devices, a mapping of a plurality of identifiers of
3 virtual private networks to corresponding views of subsets of managed objects, in the
4 form of one or more entries in a view-based access control model table that associate
5 SNMPv3 securityName values to corresponding MIB (Management Information
6 Base) Views.
- 1 4. (currently amended) A method as recited in Claim 1, further comprising the steps of
2 providing, at one of the network devices, one or more entries in a view-based access
3 control model table that associate SNMPv3 securityName values to corresponding
4 MIB (Management Information Base) Views, wherein each of the securityName

5 values is associated with a virtual private network, and wherein the corresponding
6 MIB Views represent access control policies applicable to the associated virtual
7 private networks.

- 1 5. (original) A method as recited in Claim 1, further comprising the steps of providing,
2 at one of the network devices, a mapping of a plurality of identifiers of virtual private
3 networks to corresponding views of subsets of managed objects, and wherein the
4 steps of identifying a subset of objects and providing the request with access
5 comprise the steps of.
6 determining whether the identifier from the request is in the mapping;
7 when the identifier from the request is in the mapping:
8 identifying a management information base variable referenced in the request;
9 based on one or more views referenced in the mapping, determining whether a
10 protocol operation of the request is allowed for the variable;
11 dispatching information identifying the variable and the protocol operation to
12 a code implementation of the protocol operation only when the
13 protocol operation is allowed for the variable.

- 1 6. (currently amended) A method as recited in Claim 1, further comprising the steps of
2 providing, at one of the network devices, a mapping of a plurality of identifiers of
3 virtual private networks to corresponding views of subsets of managed objects, in the
4 form of one or more entries in a view-based access control model table that associate
5 security name values to corresponding MIB (Management Information Base) Views,

6 and wherein the steps of identifying a subset of objects and providing the request with
7 access comprise the steps of[.]:
8 determining whether the identifier from the request is in the view-based access
9 control model table;
10 when the identifier from the request is in the view-based access control model table:
11 identifying a management information base variable referenced in the request;
12 based on one or more MIB Views referenced in the view-based access control
13 model table, determining whether a protocol operation of the request is
14 allowed for the variable;
15 dispatching information identifying the variable and the protocol operation to
16 a code implementation of the protocol operation only when the
17 protocol operation is allowed for the variable.

1 7. (currently amended) A method as recited in Claim 1, further comprising the steps of
2 providing, at one of the network devices, one or more entries in a view-based access
3 control model table that associate SNMPv3 securityName values to corresponding
4 MIB (Management Information Base) Views, wherein each of the securityName
5 values is associated with a virtual private network, and wherein the corresponding
6 MIB Views represent access control policies applicable to the associated virtual
7 private networks, and wherein the steps of identifying a subset of objects and
8 providing the request with access comprise the steps of[.]:
9 determining whether the identifier from the request is in the view-based access
10 control model table;

when the identifier from the request is in the view-based access control model table:
identifying a management information base variable referenced in the request;
based on one or more MIB Views referenced in the view-based access control
model table, determining whether a protocol operation of the request is
allowed for the variable;
dispatching information identifying the variable and the protocol operation to
a code implementation of the protocol operation only when the
protocol operation is allowed for the variable.

8. (original) A method as recited in Claim 1, further comprising the steps of:
providing, at a network management station that is communicatively coupled to the
network devices, a mapping of a plurality of virtual private network identifiers
to SNMPv3 securityNames;
providing, at the network management station, an executable process that associates a
virtual private network identifier with each SNMP request that is issued by the
network management station to the network devices.

9. (original) A method of controlling access of network management requests directed
to one or more network devices that participate in a virtual private network, the
method comprising the computer-implemented steps of:
receiving a request to carry out a management protocol operation, wherein the request
contains a virtual private network identifier in a security name value;
extracting the security name value and determining a protocol operation that is
embodied in the request;

8 using a view-based access control model, matching the security name value to a
9 management information base view that corresponds to the requested
10 operation;
11 processing the requested operation only if access is allowed to managed objects in the
12 management information base, based on the matching management
13 information base view.

1 10. (original) A method as recited in Claim 9, further comprising the steps of:

2 determining whether the request can be satisfied;
3 extracting the security name value from a context string in the request.

1 11. (original) A method as recited in Claim 10, wherein the matching step further

2 comprises the steps of:
3 determining whether the security name is in a view-based access control model table;
4 rejecting and returning the request when the security name is not found in the view-
5 based access control model table.

1 12. (original) A method as recited in Claim 10, further comprising the steps of:

2 determining whether the security name is in a view-based access control model table;
3 when the security name is found in the view-based access control model table:
4 identifying a management information base variable referenced in the request;
5 based on one or more views referenced in the view-based access control
6 model table, determining whether the protocol operation is allowed for
7 the variable;

8 dispatching information identifying the variable and the protocol operation to
9 a code implementation of the protocol operation only when the
10 protocol operation is allowed for the variable.

1 13. (currently amended) The method as recited in Claim 10, further comprising the steps
2 of:

3 determining whether the security name is in a view-based access control model table;
4 when the security name is found in the view-based access control model table:

5 identifying a management information base variable referenced in the request;
6 based on one or more views referenced in the view-based access control
7 model table, determining whether the protocol operation is allowed for
8 the variable;

9 dispatching information identifying the variable and the protocol operation to
10 a code implementation of the protocol operation only when the
11 protocol operation is allowed for the variable;

12 ~~using a "find first" function,~~ determining whether a virtual private network
13 identifier is referenced in the request, processing the request using
14 managed information objects in a default view when no virtual private
15 network identifier is referenced in the request, and processing the
16 request using management information objects in a view
17 corresponding to the virtual private network identifier only when a
18 virtual private network identifier is referenced in the request.

1 14. (original) A computer-readable medium carrying one or more sequences of
2 instructions for controlling access of network management requests directed to one or
3 more network devices that participate in a virtual private network, which instructions,
4 when executed by one or more processors, cause the one or more processors to carry
5 out the steps of:
6 receiving a request to carry out a management protocol operation;
7 determining an identifier of a virtual private network in the request;
8 identifying, among a plurality of managed objects, a subset of objects that requests
9 associated with the virtual private network are permitted to access; and
10 providing the request with access to only the subset of objects.

1 15. (original) A computer-readable medium as recited in Claim 14, further comprising
2 instructions which, when executed by the one or more processors, cause the one or
3 more processors to carry out the steps of providing, at one of the network devices, a
4 mapping of a plurality of identifiers of virtual private networks to corresponding
5 views of subsets of managed objects.

1 16. (currently amended) A computer-readable medium as recited in Claim 14, further
2 comprising instructions which, when executed by the one or more processors, cause
3 the one or more processors to carry out the steps of providing, at one of the network
4 devices, a mapping of a plurality of identifiers of virtual private networks to
5 corresponding views of subsets of managed objects, in the form of one or more
6 entries in a view-based access control model table that associate SNMPv3
7 securityName values to corresponding MIB (Management Information Base) Views.

1 17. (currently amended) A computer-readable medium as recited in Claim 14, further
2 comprising instructions which, when executed by the one or more processors, cause
3 the one or more processors to carry out the steps of providing, at one of the network
4 devices, one or more entries in a view-based access control model table that associate
5 SNMPv3 securityName values to corresponding MIB (Management Information
6 Base) Views, wherein each of the securityName values is associated with a virtual
7 private network, and wherein the corresponding MIB Views represent access control
8 policies applicable to the associated virtual private networks.

1 18. (original) A computer-readable medium as recited in Claim 14, further comprising
2 instructions which, when executed by the one or more processors, cause the one or
3 more processors to carry out the steps of providing, at one of the network devices, a
4 mapping of a plurality of identifiers of virtual private networks to corresponding
5 views of subsets of managed objects, and wherein the steps of identifying a subset of
6 objects and providing the request with access comprise the steps of.
7 determining whether the identifier from the request is in the mapping;
8 when the identifier from the request is in the mapping:
9 identifying a management information base variable referenced in the request;
10 based on one or more views referenced in the mapping, determining whether a
11 protocol operation of the request is allowed for the variable;
12 dispatching information identifying the variable and the protocol operation to
13 a code implementation of the protocol operation only when the
14 protocol operation is allowed for the variable.

1 19. (original) An apparatus for controlling access of network management requests
2 directed to one or more network devices that participate in a virtual private network,
3 comprising:
4 means for receiving a request to carry out a management protocol operation;
5 means for determining an identifier of a virtual private network in the request;
6 means for identifying, among a plurality of managed objects, a subset of objects that
7 requests associated with the virtual private network are permitted to access;
8 and
9 means for providing the request with access to only the subset of objects.

1 20. (original) An apparatus controlling access of network management requests
2 directed to one or more network devices that participate in a virtual private
3 network, comprising:
4 a network interface that is coupled to the data network for receiving one or more
5 packet flows therefrom;
6 a processor;
7 one or more stored sequences of instructions which, when executed by the
8 processor, cause the processor to carry out the steps of:
9 receiving a request to carry out a management protocol operation;
10 determining an identifier of a virtual private network in the request;
11 identifying, among a plurality of managed objects, a subset of objects that
12 requests associated with the virtual private network are permitted
13 to access; and

14 providing the request with access to only the subset of objects.

1 21. (new) A method of controlling access of network management requests directed
2 to one or more network devices that participate in one or more virtual private
3 networks, the method comprising the computer-implemented steps of:
4 receiving a request to carry out a SNMP (Simple Network Management Protocol)
5 operation directed to one or more managed objects from a MIB
6 (Management Information Base) associated with one or more network
7 devices that participate in multiple virtual private networks;
8 determining, from the request, an identifier of a particular virtual private network
9 of the multiple virtual private networks;
10 identifying, among a plurality of managed objects from a MIB associated with a
11 network device from the one or more network devices that participate in
12 the multiple virtual private networks, a subset of managed objects that
13 requests associated with the particular virtual private network are
14 permitted to access; and
15 in response to the request, providing access to only the subset of managed objects.